



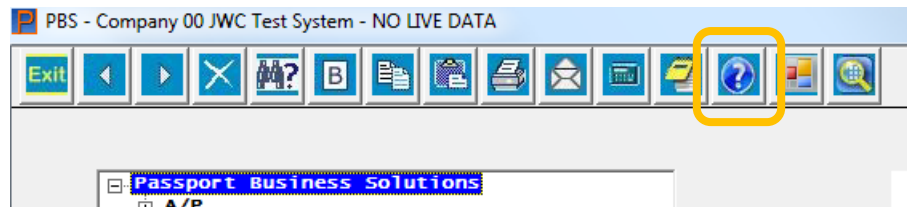
Tips & Tricks #46 – Security Options in Passport Products

This article is offered as a two-part series covering access controls and security features within Passport Business Solutions (PBS), PBS Manufacturing and CashPoint accounting systems. This article covers logins, passwords and the resulting access to different functions within the software. Upcoming Part 2 will deal with security and protection issues for the accounting system reports and protection for special fields.


Security is an issue that confronts us almost daily in reports, news and technology tool availability and so knowing the major elements of security provided by the Passport accounting system will prove useful. This discussion will highlight areas where security options are available and where there are choices to be made to protect the system. Fine details may not be discussed but reference to appropriate documentation will be made. As much of this is related to system setup, it can only be acted on if you are an Administrative user. We will cover options that are available and provide some talking points to discuss with the Admin responsible where appropriate.

Where to find detailed information

The manual that covers most of the functions described here is the PBS Administration manual and is available by clicking the Help icon at the top of the main screen:



This will open the documentation selection screen:



Administrative and User Documentation

Click on the module name to access the documentation for that module.
All documentation is in HTML format, except when noted is in Acrobat PDF format.

Administrative Documentation	
PBS Administration	
V12.07 Vision Installation Guide (PDF)	
SQL Installation Guide (PDF)	
EZ Convert (PDF)	
CashPoint (PDF)	
Passport Query Builder User Guide (PDF)	
Passport Query Builder Configuration Guide (PDF)	
Accounting and Distribution Modules Field Definition Guide (PDF)	
Manufacturing Field Definition Guide (PDF)	
Data Import Manager	
Master Key Conversion (PDF)	
Thin Client Configuration (PDF)	
XDBC (ODBC) Configuration (PDF)	

PBS User Documentation	
Accounting and Distribution	Manufacturing
System	Customer Orders
Accounts Payable	Capacity Requirements Planning

The Admin manual link shown above is an online display (i.e.,HTML5 page) with an indexed set of chapter headings referred to below. Because of the sensitive/setup nature of the subjects discussed, the entire Administrative Documentation group of documents is only available to users with Admin privileges in PBS. For others going to this site, the page display starts with the PBS User Documentation seen below the Administration section.

In addition to the PBS Admin documentation, the Control File Maintenance function in Accounts Payable or Payroll is referenced as the source of information on specific setup information for these modules. The documentation for these topics is located in the AP or PR User documentation under the Control File Maintenance chapter.

Introduction

Passport is not discussing or advising you on issues related to your Operating System/Windows security or security issues concerning your network, or anti-malware issues. This is something better left to the computer and IT/network gurus who support you. However, as indicated in our last piece about what to do about what you don't know, if you are uncomfortable with your ability to understand or tackle some of these computer/network/malware security issues, please contact Passport or your Passport Partner and we will do our very best to point you to the right people.

Access Control - Logins, passwords and menus

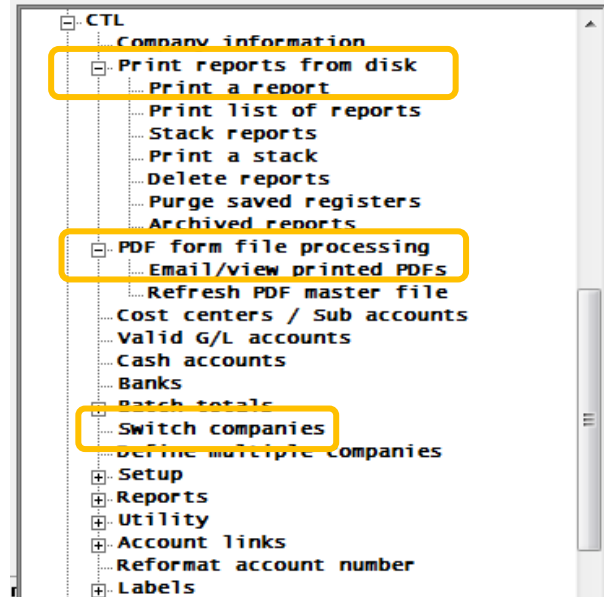
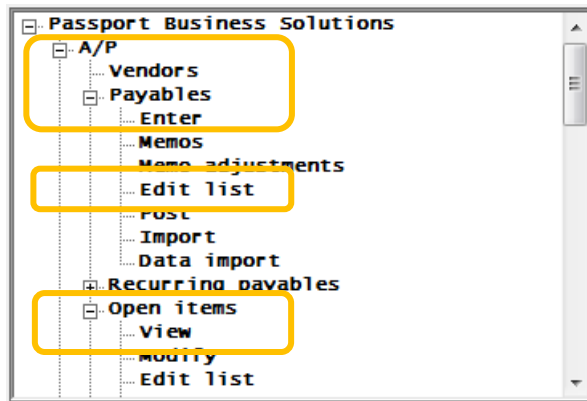
The Operating System you use, (MS Windows, MS SQL or LINUX/UNIX) requires a log in to gain access to any portion of the computer and network system. What portions of the system are made available, *resources* such as printers, and network drives and specific kinds of information, are determined and set up by the system's administrator.

By the same token, when logging in to the PBS accounting system with an ID and password, you are given privileges and access to certain functional areas assigned by the person(s) who set up your accounting system. They are also the ones who created and maintain the logins and passwords, (These logins and passwords have no relation to the computer logins and passwords.) The PBS login uses a three-character ID (1 to 3 alphanumeric characters) with any alpha characters converted to upper case. These are by convention, frequently the individual user's initials. The PBS password is 6-10 characters (alphanumeric) and must include at least two of the following three types: upper case, lower case and numeric. This level of password is considered medium-strong and can be made stronger by including special characters in addition to the other 3 types.

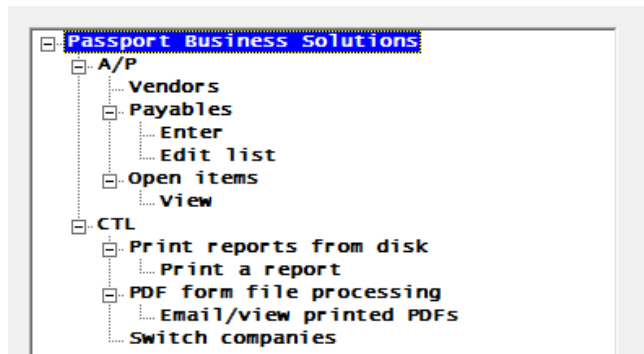
The way Passport exerts control on what you can and can't do is by allowing the system admin to customize the menu of accounting functions and reports that each user or group of users has access to. If the menu entry for a function doesn't exist for a user, they simply can't execute the function. For example, even though there may be half a dozen different applications available within your Passport system (e.g., AP, AR, OE, IC, PR GL), the Accounts Payable clerk, may only be given access to those areas of the accounting that are directly related to the areas needed to work in. For instance, your access menu may only have the vendor invoice entry function (voucher creation), the print edit list function and post transactions function on the menu. Further, although clearly accessing vendor information is necessary for processing vouchers, if there is company policy about who controls the selection and entry of vendor information, the menu entry that allows the *Maintenance* of the Vendor Master file may be restricted.

The examples given above involve some rather significant menu and sub-menu security restrictions. As a possible contrast, the payroll clerk may have access to anything related to payroll within that module, but access to nothing else on the system. The controller for the company will likely have access to the complete accounting system, but may be the only person with access to the General Ledger portions of the system and corresponding menu functions.

PBS controls access to these various functional area by having two levels of user access to the system – '*administrator*' and '*general user*'. An '*administrator*' has access to all functions in PBS and this includes adding and modifying what the '*general user*' can do. Since the menu of functions presented to a user is the only means by which they can access a function, the administrator controls access by selecting which menu items a user will have. Here are two parts of the menu for an admin user for a portion of the PBS functions:



The highlighted items are the subset that might be assigned to a junior clerk and shows more than half of the possible functions available to an admin user have been eliminated for this user. If we wanted to limit our AP clerk to just entering vouchers and running the edit list and viewing Open Items in AP and printing reports and switching companies in the Control module, then their (personalized) menu would look like this:



The important pre-requisite for you, as the admin/menu designer, is to organize your thoughts around who should be able to do what functions. Or, from the point of view of setup, who should be restricted to doing only what. As an example of the decision-making process, you could consider that having an employee both entering *and* posting transactions involves a formal lack of oversight/review for those transactions. In many smaller company situations this may be acceptable; but in some companies, this could actually violate Sarbanes-Oxley rules of formal review. Fixing this could entail assigning one person the entry/edit list function and another person the posting function. Similarly, generally not all employees should have access to the Payroll system, and possibly the General Ledger, and this selective menu setup will produce this kind of control.

This method of controls allows you to limit user access to the functions and the data they generate by first defining different job types/work types e.g., 'AP Clerk', 'Payroll Supervisor', 'Assistant Controller' etc., and then assigning specific functions (menu entries) to each of the types.

Details on the setup of Users and assigning their Menus is given in the 'PBS Users' and 'PBS Menus' chapters in the Administration Guide referenced above.

One important note, as we have mentioned, many functions in the CTL Menu main menu and in the Master information sub-menu in each application allow changes be made that can affect the fundamental operation of the system. These should only be available to an admin user. You could/should have some users defined as *admin users* and the remainder as *general users* whose menu only differs from the full admin menu by removing the admin functions. A more restrictive implementation can have menus by work type as described above but at a minimum there should be an explicit differentiation between a small group of admin users and the rest. (Some small companies may have only 2 or 3 users who are all equally empowered to make changes, and this would be a situation where everyone would be assigned as admin.)

One additional note: In a multi-company environment where Passport has data for multiple companies (legal entities), the User/Menu protection function can be set up differently for each company and user combination. That means that each user can be allowed or disallowed from even accessing some of the companies and/or can have different privileges within each company. One example might be a retail outfit owning the building in which they conduct business. They run the retail business as one company and run the "real-estate" business (rents for, and repairs/maintenance for the building) as another. Only some of the users will be involved with expense transactions for the real-estate company and as a result user access for taking care of AP transactions may be different for the two companies.

We hope you found Part 1 of this Tips & Tricks useful.

Part 2 will cover how Passport provides security and protection for reports and special fields.